Comments and Recommandations on the PSS Version 3 Proposal

Date: April 17, 2003

Review Committee:
John Forrestal, Nick Friedman, Jon Hawkins, Marty Knott, Jonathan Lang, Mohan Ramanathan, Josh Stein

The review committee would like to thank the speaker(s) and group of designers for the effort in enlightening the committee members on their proposal for the next generation PSS system.

The committee was asked to review the presentation based on the following criterion:

- **Are we doing the right thing by migrating our standard PSS implementation from the existing Generation-1 systems to a Generation-3 system?**
- **Are we focusing on the right issues?**
- **Assess the different technical options for the Generation-3 system.**
- **Provide feedback and guidance on how we should move forward.**
- **Provide feedback and guidance on anything else you feel is pertinent.**

Summarized below is the general consensus.

The philosophy behind the migration from PSS v1 to PSS v3 was addressed. The advantage of migrating to a 3-chain system from the current 2-chain system (in use in most of the beamlines) was questionable. While a partial majority of the committee felt a desire to separate the control functionality from the emergency shutdown it was not clear whether the issues related to main philosophy of a 3-chain system has been analyzed.

The fact that the current hardware will be obsolete in a short time requires addressing possible upgrade path. The natural desire at this stage would be to address the shortcomings of the current system and design a new system. The committee feels that the design group has taken this approach.

Some of the reasons given for the migration to the new 3-chain system were not justifiable. For example the issue related to shortening of PSS validation would take more than 5 years (if at all) to materialize. While the idea of automating the validation process, it was not clear whether the effort to make the automation process is more resource hungry than the current V & V process. The break-even point may be in the distant future.

Having addressed the issues related to the negative aspects of migration, overall the committee felt that the direction of moving to a 3-chain system has its advantages. The burden of making the decision will be on the management only.

It is clear that the ESS groups desire is to proceed with the PSS v3 with three chains. Based on these circumstances here are some points in favor of such move:

The separation of control and command from the emergency shutdown is a good idea. This will definitely simplify the chain A and Chain B, the main two emergency shutdown chains. In the eyes of the DOE the credit for validation will be for just these two safety chains. Additionally moving the control functionality to a third independent chain, where no safety credit is taken, has the advantages on high level of integration to the APS control system, namely EPICS for monitoring and controlling. This was one sore issue related to the current PSS v1, in that the EPICS interface was minuscule.

The chain C has the advantage of not requiring a rigorous validation, however it will be prudent in the initial stages to have a validation process.

Much emphasis should be given from the beginning to integrate EPICS interface into the chain C, as time will reveal the advantages of using the full functionality of EPICS interface of logging and analysis.

The committee was presented with a few options for the hardware platform for the new system. It was a unanimous decision, that the chain C should be a PLC based and not a PC based system. As to the choice of the HMI for the beamline, there is a desire to use a Wonder Ware based touch screen due to the advantages of providing better control of the screens needed for the beamline. The choice of using Wonder Ware based touch screens or say Panelview touch screen will be left to the designers.

Issues related to the choice of PLC vendor for the three chains were discussed. Use of same type of PLC for all three chains will help in reduction of spares inventories and adds to having to deal with only one vendor as against maybe, three! While selecting same type of PLC for all chains may be desirable, the APS SAD clearly has taken credit in the past for the choice of different vendor hardware for the two chains. This issues needs to be addressed. It may not be difficult to address this, however it must be addressed at the earliest.

It is clear that the designers are already aware of the importance of having the EPICS interface built into the new PSS for the beginning. We would like to stress that the EPICS interface can be advantageous during the earlier stages of PSS installation and validation.

If the preferred choice for the HMI interface is the Wonder Ware Thin Client devices, the Ethernet link between the server and the clients on the beamline has to be on dedicated private networks for each beamline.

The committee would like to see this new system implemented in beamline and adequate testing be done before handing over to the users. The ESS group has the advantage of using the Sector 30 IXS beamline as a test bed, as this beamline stations will be built by

December 2003 while the first beam in the station will not be until September 2004. In addition this beamline is funded by BES and is managed by APS members.

Listed below are view and suggestions of specific issues:

- When Jordi Roglands (then Reactor Analysis) performed an analysis of the ACIS in 1994 little or no credit was taken for the failure modes of the PLC's when in fact the vast majority of PLC failures are detectable or can be compensated for by additional components (external watchdogs, monitoring component feedback, etc.). Also, very conservative estimates were used for software reliability. Naturally the conclusion of having a hardwire chain benefited the overall *shutdown* reliability of the system. If, in the final analysis, keeping two different types of PLC's means a hardwired chain is not necessary, by all means use diverse processors. However, having the same PLC's does not necessitate a hardwired chain (TJ Lab's CEBAF for example). Also, SNS is designing their system based on two AB Controllogix systems without hardwired backup. The question of diversity in safety systems is a sound practice but in the case of the PSS the improvement in PFD seems minimal at best. Thus, using Allen Bradley PLC's for both PSS safety chains seems reasonable. The reduced inventory that results from using only one brand of PLC is a second order effect, but a positive one.

- The addition of a third processor having access to all of the I-O of the two ESD chains opens the door to a scheme to monitor and alarm on differing states of various important inputs. All input which are supposed to react the same for both ESD chains, a door switch for example, would be monitored by chain C and if they were different for any appreciable time, an alarm would sound. The meaning of the alarm is a potential loss-of-redundancy event, which by the way, is a reportable event to the DOE. Loss-of-redundancy is a serious situation when it involves a critical device such as a door or shutter since one chain could be content thinking that a door or shutter is always closed when, in fact, it may be open. The reliability equations take into account the *mission time* of field devices and this addition will shorten the mission time from 12 months (the inter-validation time) to the much shorter periodic execution time. Since chain C is not likely to be considered a fully validated (trusted) system, this addition will produce no *official* safety credit in the eyes of the DOE, but will produce real safety and help in maintenance.

- Even though the quality of the search is ultimately a function of the searcher, search confirmation buttons are discussed in the interlock order guidance, therefore they should be included as part of the safety PLC's rather than Chain C. There is probably a DOE mandate that the interlock system monitor and enforce the search process. Now the DOE order is written under the assumption that a set of redundant interlock systems is built, not a *helper* system (PSS-3's chain C), so the order must be interpreted that the primary interlock system(s) must do this job, not an *untrusted system*. For this reason ESD chains should do this task. Perhaps a combination methodology could be adopted, with Chain A (or A&B) do the *enforcement* mandated by DOE (making sure the buttons are pressed in the proper order) and have the *guidance* performed by chain C (lighting prompting lights in order).

- Although a method of emergency egress was listed for the hutches, there was no mention of emergency entrance buttons.

- The EPICS variable names from beamline to beamline should be standardized and have some description of the function i.e. Something like *beamline:AShutterOpen*.

- The automated testing as described raises some logistical issues. It is the understanding that the testing computer (mounted on a cart) will be connected by removable cables to each 15u and the racks on the mezzanine. Unless these cables are permanently installed (disconnected when not in use) cables will have to be run each time the testing computer is connected, typically on the floor to the various locations and over the rail to the mezzanine. When determining total validation time saved, the effort to run these cables must be taken into account.

- Automated testing was discussed but the details were put off to another time. Because it is hardware intensive, decisions must be made early on to what will be implemented. It is also something that will be closely looked at by review committees therefore compelling reasons must be given as well as realistic expectations in terms time saved and confidence that the systems are being correctly tested. It is difficult to see how safety credit can be taken for a using a test system that is not under the same level of configuration control as the safety PLC's. These are concerns but not necessarily show stoppers.

- When the automated system is connected it must be guaranteed that the front end shutters cannot be opened. A recommended choice is a key operated selector switches installed to disconnect the shutters from PSS control (similar to the ACIS's Controlled Equipment interfaces) before the automated system can be activated.

- The methods used to make a non-invasive attachment of the test processor should be assessed carefully for their failure methods. This is critical to the success of the automated testing.

The committee recognizes the mammoth task ahead for the designers …